REMARKS

Claims 1-69 are pending in the application. Applicants have amended claims 42 and 51. By these amendments, Applicants do not acquiesce to the propriety of any of Examiner's rejections. Indeed, these amendments are merely to correct typographic errors. These amendments, therefore, do not disclaim any subject matter to which the Applicants are entitled. *Cf. Warner Jenkinson Co. v. Hilton-Davis Chem. Co.*, 41 USPQ2d 1865 (U.S. 1997). Indeed, these amendments are not intended to in any way narrow the subject the matter for which a patent is sought.

Applicants have attached Appendix A pursuant to 37 C.F.R. 1.121(c). Appendix A is entitled "Version with Markings to Show Changes Made" and is a marked-up version of the prior pending claims illustrating claim amendments made in the present reply.

Rejection Under 35 U.S.C. § 112: Indefiniteness

The Examiner rejected claims 14, 18, 27-29, and 34 under 35 U.S.C. § 112 ¶ 2 as being indefinite because they use the term "unique" or "uniquely" and that term is a "relative term." Paper 14, p. 3, paragraph 6. Applicant respectfully traverses these rejections.

Applicants fail to appreciate, in the context of the claims, the Examiner's statement that "unique" is a "relative term." Examiner's explanation that "'unique' is an infinitive range" only further obfuscates.

Accepting, *arguendum*, that "unique" is a relative term, it is unclear why the condition of being a "relative term" would make the use of the word "unique" a basis for rejecting the claim. Applicants respectfully suggest that relative terms indicate relation and thus point out and distinctly claim the subject matter which applicant regards as the invention. Applicants reasonably anticipate that the terms of the claim, including any relative terms, will be read within the context of the claim and the specification.[1]

---

[1] Applicants note that (as of February 16, 2004) since 1976, 23,311 U.S. patents have issued with the words "unique" or "uniquely" in the claims. See http://patft.uspto.gov/netacgi/nph-

(Footnote cont'd on next page.)

The Examiner rejected claims 42, 51, 54, 59-62, and 64 under 35 U.S.C. § 112 ¶ 2 as being indefinite because they use the term "sensitive" and that term is a "relative term." Paper 14, p. 3, paragraph 7. Applicant respectfully traverses these rejections.

Applicants note that claims 59-62 and 64 do not contain the term "sensitive." Applicants respectfully thus request that the rejection of these claims be withdrawn.

Applicants fail to appreciate, in the context of the claims, the Examiner's statement that "sensitive" is a "relative term." Examiner's explanation that "sensitive has a wide, endless range" does not clarify. Applicants respectfully suggest that relative terms indicate relation and thus point out and distinctly claim the subject matter which applicant regards as the invention. Applicants reasonably anticipate that the terms of the claim, including any relative terms, will be read within the context of the claim.

Applicants additionally note that the claim language simply recites "sensitive" without calling out a particular degree of sensitivity. Thus, there is no need to determine a degree of sensitivity to understand the scope of the claims.

Applicants do not see any legal basis for rejecting claims based on language that is argued by the Examiner to be relative. Applicants note that on pages 9 and 11 of the office action the Examiner asserts that other art teaches something with regard to "sensitive data." Paper 14, pp. 9, 11. It is thus inconsistent for the Examiner to assert that "sensitive" is indefinite, because its use by the Examiner in rejecting the claim indicates that the Examiner

---

(Footnote cont'd from previous page.)

Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2Fsearch-bool.html&r=0&f=S&l=50&TERM1=unique&FIELD1=ACLM&co1=OR&TERM2=uniquel y&FIELD2=ACLM&d=ptxt for the full results of the search. Applicants respectfully suggest that this indicates that word "unique" is not necessarily an indefinite term.

believes that the Examiner knows what is claimed.[2] Applicants therefore respectfully request that these rejections be withdrawn.

Rejection Under 35 U.S.C. 102(e): Okumara et al. (U.S. Patent No. 6,553,493)

Examiner rejected claims 1-4, 7-13, and 59-69 under 35 U.S.C. § 102(e) as "being anticipated by Okumara et al. (U.S. Patent 6,553,493)." Paper No. 14, page 4, paragraph 8. Applicant respectfully traverses these rejections.

To properly maintain a rejection under Section 102, the Examiner must show that each and every limitation of the claims of the present invention are anticipated by the alleged prior art. *See In re Bond*, 15 USPQ2d 1896 (Fed. Cir. 1991).

The cited reference, *Okumara*, fails to anticipate the claims of the present invention because it does not disclose each and every element of the present invention as claimed.

With regard to independent claim 1, what is claimed is:

1.   A remotely accessible secure cryptographic system for storing a plurality of private cryptographic keys to be associated with a plurality of users, wherein the cryptographic system associates each of the plurality of users with one or more different keys and performs cryptographic functions for each user using the associated one or more different keys without releasing the plurality of private cryptographic keys to the users, the cryptographic system comprising:

a depository system having at least one server which stores a plurality of private cryptographic keys and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users and

---

[2] Applicants additionally note that (as of February 16, 2004) since 1976, 48,137 U.S. patents have issued with the word "sensitive" in the claims. See http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2Fsearch-bool.html&r=0&f=S&l=50&TERM1=sensitive&FIELD1=ACLM&col=AND&TERM2=&FIELD2=ACLM&d=ptxt for the full results of the search. Applicants respectfully suggest that this indicates that word "sensitive" is not necessarily an indefinite term.

each of the multiple users is associated with one or more different keys from the plurality of private cryptographic keys;

an authentication engine which compares authentication data received by one of the multiple users to enrollment authentication data corresponding to the one of multiple users and received from the depository system, thereby producing an authentication result;

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users, performs cryptographic functions on behalf of the one of the multiple users using the associated one or more different keys received from the depository system; and

a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine.

– Claim 1

Applicants note that the Examiner has not explained how each and every limitation of the claim is present. Moreover, *Okumara* does not contain all of the elements of the claims. Furthermore, Applicants note that Examiner's assertion that *Okumara* teaches "enrollment authentication data" is incorrect. The digital certificates of *Okumara* are generated by the system. ("[A] digital certificate [is] issued to the entity." Abstract, *Okumara*) In contrast, the claim calls for "enrollment authentication data" which "identifies one of the multiple users." A comparison of "authentication data ... to enrollment authentication data" yields "an authentication result." *Okumara* does not teach this. Thus, the cited reference does not teach at least this element of the claim. Thus, *Okumara* does not anticipate claim 1.

With regard to independent Claim 2 and dependent claims 3-4 and 7-9 what is claimed, in relevant portion is:

2. A remotely accessible secure cryptographic system, comprising:

a depository system having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;

an authentication engine which compares authentication data received by one of the multiple users to enrollment authentication data corresponding to the one of multiple users and received from the depository system, thereby producing an authentication result;

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users, performs cryptographic functions on behalf of the one of the multiple users using at least said private key received from the depository system; and

a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine.

– Claim 2.[3]

Examiner is obliged to explain the basis for rejection, and, in particular, how the cited reference teaches each and every element of the claim. The Examiner has not done this. Applicants further note that not all of the elements of the claims are taught by *Okumara*. In particular, Applicants note that Examiner's assertion that *Okumara* teaches "enrollment authentication data" is incorrect. The digital certificates of *Okumara* are generated by the system. ("[A] digital certificate [is] issued to the entity." Abstract, *Okumara*) In contrast, the claim calls for "enrollment authentication data" which "identifies one of the multiple users." A comparison of "authentication data ... to enrollment authentication data" is made and "an authentication result" is produced. *Okumara* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

With regard to independent Claim 10 and dependent claims 11-13, what is claimed, in relevant portion is

10.   A method of facilitating cryptographic functions, the method comprising:

associating a user from multiple users with one or more keys from a plurality of private cryptographic keys stored on a secure server;

---

[3] Claims 3-4 and 7-9 depend on, and therefore include the limitations of, claim 2.

receiving authentication data from the user;

comparing the authentication data to authentication data corresponding to the user, thereby verifying the identity of the user; and

utilizing the one or more keys to perform cryptographic functions without releasing the one or more keys to the user.

– Claim 10.[4]

The cited reference does not contain every element of this claim. The Examiner has not pointed out how the reference teaches each and every element of this claim. In particular, Applicants note that *Okumara* doesn't teach "receiving authentication data from the user." The digital certificates of *Okumara* are generated by the system. ("[A] digital certificate [is] issued to the entity." Abstract, *Okumara*) In contrast, the claim calls for "receiving authentication data from the user." *Okumara* does not teach this. Thus, *Okumara* does not teach every element of claim 10 or dependent claims 11-13.

With regard to independent claim 59 and dependant claims 60-64, what is claimed, in relevant portion, is:

59.   A secure authentication system, comprising:

a plurality of authentication engines, wherein each authentication engine receives enrollment authentication data designed to uniquely identify a user to a degree of certainty, each authentication engine receives current authentication data to compare to the enrollment authentication data, and wherein each authentication engine determines an authentication result; and

a redundancy system which receives the authentication results of at least two of the authentication engines and determines whether the user has been uniquely identified.

– Claim 59.[5]

---

[4] Claims 11-13 depend on, and therefore include the limitations of, claim 10.

The cited reference does not contain every element of this claim. The Examiner does not explain how the reference teaches each and every element. In particular, Applicants note that Examiner's earlier assertion that *Okumara* teaches "enrollment authentication data" is incorrect. The digital certificates of *Okumara* are generated by the system. ("[A] digital certificate [is] issued to the entity." Abstract, *Okumara*) In contrast, the claim calls for "enrollment authentication data" which "designed to uniquely identify a user." A comparison of "current authentication data ... to enrollment authentication data" is made and "an authentication result" is produced. *Okumara* does not teach this. Thus, *Okumara* does not teach every element of independent claim 59 and dependent claims 60-64.

With regard to independent claim 65 and dependant claims 66-69, what is claimed, in relevant portion, is:

65.   A trust engine system for facilitating authentication of a user, the trust engine system comprising:

a first trust engine comprising a first depository, wherein the first depository includes a computer accessible storage medium which stores portions of enrollment authentication data;

a second trust engine located at a different geographic location than the first trust engine and comprising:

a second depository having a computer accessible storage medium which stores portions of enrollment authentication data,

an authentication engine communicating with the first and second depositories and which assembles at least two portions of enrollment authentication data into a usable form, and

a transaction engine communicating with the first and second depositories and the authentication engine,

---

(Footnote cont'd from previous page.)

[5] Claims 60-64 depend on, and therefore include the limitations of, claim 59.

wherein when the second trust engine is determined to be available to execute a transaction, the transaction engine receives authentication data from a user and forwards a request for the portions of enrollment authentication data to the first and second depositories, and wherein the authentication engine receives the authentication data from the transaction engine and the portions of the enrollment authentication data from the first and second depositories, and determines an authentication result.

– Claim 65.[6]

The cited reference does not contain every element of this claim. For example, the Examiner has not explained which element of *Okumara* corresponds to each of the elements in the claim. Examiner bafflingly simply states for this independent claim "As rejected on the same rationale as applied to claim 1." Claim 65 is distinct from Claim 1 and a rejection requires an explanation. Applicants note that, for example, *Okumara* does not teach "wherein the authentication engine ... determines an authentication result." For example, the Examiner relies on the digital certificates in the examiner's comments regarding claim 1, but the digital certificates of *Okumara* are generated by the system. ("[A] digital certificate [is] issued to the entity." Abstract, *Okumara*) Consequently, the certificates are produced so that another system (for example a user) can perform authentication or for other reasons (Applicant notes that *Okumara* does not teach that the certificates must be put to any use. Thus, *Okumara* does not teach every element of claim 65.

Rejection Under 35 U.S.C. 102(e): Patel et al. (U.S. Patent No. 6,438,690)

Examiner rejected claims 14-35 under 35 U.S.C. § 102(e) as "being anticipated by Patel et al. (U.S. Patent 6,438,690)." Paper No. 14, page 8, paragraph 9. Applicant respectfully traverses these rejections.

---

[6] Claims 66-69 depend on, and therefore include the limitations of, claim 65.

To properly maintain a rejection under Section 102, the Examiner must show that each and every limitation of the claims of the present invention are anticipated by the alleged prior art. *See In re Bond*, 15 USPQ2d 1896 (Fed. Cir. 1991).

The cited reference, *Patel*, fails to anticipate the claims of the present invention because it does not disclose each and every element of the present invention as claimed.

With regard to independent claim 14 and dependent claims 15-29, what is claimed in relevant portion is:

14.   An authentication system for uniquely identifying a user through secure storage of the user's enrollment authentication data, the authentication system comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of enrollment authentication data; and

an authentication engine which communicates with the plurality of data storage facilities and comprises:

a data splitting module which operates on the enrollment authentication data to create portions,

a data assembling module which processes the portions from at least two of the data storage facilities to assemble the enrollment authentication data, and

a data comparator module which receives current authentication data from a user and compares the current authentication data with the assembled enrollment authentication data to determine whether the user has been uniquely identified.

– Claim 14.[7]

---

[7] Claims 15-29 depend on, and therefore include the limitations of, claim 14.

The cited reference does not contain every element of this claim. Applicants note that the Examiner has not explained how each and every limitation of the claim is present. In particular, Applicants note that Examiner doesn't even assert that *Patel* teaches "a plurality of data storage facilities." One limitation of claim 14 is "a plurality of data storage facilities." *Patel* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

With regard to independent Claim 30 and dependent claims 31-35 what is claimed, in relevant portion is:

> 30.   A cryptographic system comprising:
>
> a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of cryptographic keys; and
>
> a cryptographic engine which communicates with the plurality of data storage facilities and comprises
>
> > a data splitting module which operates on the cryptographic keys to create portions,
> >
> > a data assembling module which processes the portions from at least two of the data storage facilities to assemble the cryptographic keys, and
> >
> > a cryptographic handling module which receives the assembled cryptographic keys and performs cryptographic functions therewith.

– Claim 30.[8]

The Examiner has not explained how each and every limitation of this claims is present in *Patel*. Furthermore, the cited reference does not contain every element of this claim. In particular, Applicants note that Examiner doesn't even assert that *Patel* teaches "a plurality of data storage facilities." One limitation of claim 30 is "a plurality of data storage

---

[8] Claims 31-35 depend on, and therefore include the limitations of, claim 30.

facilities." *Patel* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

Rejection Under 35 U.S.C. 102(b): Schneier et al. (U.S. Patent No. 5,768,382)

Examiner rejected claims 36-58 under 35 U.S.C. § 102(b) as "being anticipated by *Schneier* et al., U.S. Patent 5,768,382." Paper No. 12, page 3, first paragraph. Applicant respectfully traverses this rejection.

To properly maintain a rejection under Section 102, the examiner must show that each and every limitation of the claims of the present invention are anticipated by the alleged prior art. *See In re Bond*, 15 USPQ2d 1896 (Fed. Cir. 1991).

The cited reference, *Schneier*, fails to anticipate the claims of the present invention because it does not disclose each and every element of the present invention as claimed.

36. A method of storing authentication data in geographically remote secure data storage facilities thereby protecting the authentication data against comprise of any individual data storage facility, the method comprising:

receiving authentication data at a trust engine;

combining at the trust engine the authentication data with a first substantially random value to form a first combined value;

combining the authentication data with a second substantially random value to form a second combined value;

creating a first pairing of the first substantially random value with the second combined value;

creating a second pairing of first substantially random value with the second substantially random value;

storing the first pairing in a first secure data storage facility; and

storing the second pairing in a second secure data storage facility remote from the first secure data storage facility.

– Claim 36.

The Examiner has not explained how each and every element of the claim is taught by the cited reference. In particular, Applicants note that Examiner doesn't even assert that *Schneier* teaches "storing the second pairing ... remote from the first secure data storage facility." One limitation of claim 36 is "storing the second pairing ... remote from the first secure data storage facility." *Schneier* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

With regard to independent Claim 37 and dependent claims 38-44, what is claimed, in relevant portion is:

37.   A method of storing authentication data comprising:

receiving authentication data;

combining the authentication data with a first set of bits to form a second set of bits;

combining the authentication data with a third set of bits to form a fourth set of bits;

creating a first pairing of the first set of bits with the third set of bits;

creating a second pairing of the first set of bits with the fourth set of bits;

storing one of the first and second pairings in a first computer accessible storage medium; and

storing the other of the first and second pairings in a second computer accessible storage medium.

– Claim 37.[9]

The cited reference does not contain every element of this claim. In particular, Applicants note that Examiner doesn't even assert that *Schneier* teaches "storing the other of the first and second pairings in a second computer accessible storage medium." One limitation of claim 37 is "storing the other of the first and second pairings in a second computer accessible storage medium." *Schneier* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

---

[9] Claims 38-44 depend on, and therefore include the limitations of, claim 37.

With regard to independent Claim 45, what is claimed, in relevant portion is:

45.   A method of storing cryptographic data in geographically remote secure data storage facilities thereby protecting the cryptographic data against comprise of any individual data storage facility, the method comprising:

   receiving cryptographic data at a trust engine;

   combining at the trust engine the cryptographic data with a first substantially random value to form a first combined value;

   combining the cryptographic data with a second substantially random value to form a second combined value;

   creating a first pairing of the first substantially random value with the second combined value;

   creating a second pairing of the first substantially random value with the second substantially random value;

   storing the first pairing in a first secure data storage facility; and

   storing the second pairing in a secure second data storage facility remote from the first secure data storage facility.

– Claim 45.

The cited reference does not contain every element of this claim. Applicants note that the Examiner fails to provide an explanation of how each element of Claim 45 is present in *Schneier*. In particular, Applicants note that Examiner doesn't even assert that *Schneier* teaches "storing the second pairing ... remote from the first secure data storage facility." One limitation of the claim is "storing the second pairing ... remote from the first secure data storage facility." *Schneier* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

With regard to independent claim 46 and dependent claims 47-53, what is claimed, in relevant portion, is:

46.   A method of storing cryptographic data comprising:
   receiving authentication data;

combining the cryptographic data with a first set of bits to form a second set of bits;

combining the cryptographic data with a third set of bits to form a fourth set of bits;

creating a first pairing of the first set of bits with the third set of bits;

creating a second pairing of the first set of bits with the fourth set of bits;

storing one of the first and second pairings in a first computer accessible storage medium; and

storing the other of the first and second pairings in a second computer accessible storage medium.

– Claim 46.[10]

The cited reference does not contain every element of this claim. Applicants note that the Examiner fails to provide an explanation of how each element of Claim 46 is taught by *Schneier*. In particular, Applicants note that Examiner doesn't even assert that *Schneier* teaches "storing the other of the first and second pairings in a second computer accessible storage medium." One limitation of the claim is "storing the other of the first and second pairings in a second computer accessible storage medium." *Schneier* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

With regard to independent claim 54 and dependent claims 55-58, what is claimed, in relevant portion, is:

54. A method of handling sensitive data in a cryptographic system, wherein the sensitive data exists in a useable form only during actions employing the sensitive data, the method comprising:

receiving in a software module, substantially randomized sensitive data from a first computer accessible storage medium;

---

[10] Claims 47-53 depend on, and therefore include the limitations of, claim 46.

receiving in the software module, substantially randomized data from a second computer accessible storage medium;

processing the substantially randomized sensitive data and the substantially randomized data in the software module to assemble the sensitive data; and

employing the sensitive data in a software engine to perform an action, wherein the action includes one of authenticating a user and performing a cryptographic function.

– Claim 54.[11]

The cited reference does not contain every element of this claim. For example, the Examiner has not explained which element of *Schneier* corresponds to each of the elements in the claim. In particular, Applicants note that Examiner doesn't even assert that *Schneier* teaches "processing ... to assemble the sensitive data." One limitation of claim 54 is "processing ... to assemble the sensitive data." *Schneier* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

Rejection Under 35 U.S.C. 103(a): Okumara et al. (U.S. Patent No. 6,553,493), and further [sic] in view of Schneier et al. (U.S. Patent No. 5,768,382)

Examiner rejected claims 5 and 6 under 35 U.S.C. § 103(a) as "being unpatentable over Okumura, et al., and further in view of Schneier, et al." Paper No. 14, page 12, paragraph 11. Applicant respectfully traverses this rejection.

To properly maintain a rejection under 35 U.S.C. § 103, the prior art must have suggested to those of ordinary skill in the art that they should make the claimed composition or device or carry out the claimed process, with a reasonable expectation of success. Both the suggestion and the reasonable expectation of success must be adequately founded in the prior

---

[11] Claims 55-58 depend on, and therefore include the limitations of, claim 54.

art and not in the Applicant's disclosure. *See In re Vaeck*, 20 USPQ2d 1438, 1442 (Fed. Cir. 1991).

With regard to dependent claims 5 and 6 what is claimed, in relevant portion, is:

2.   A remotely accessible secure cryptographic system, comprising:

a depository system having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;

an authentication engine which compares authentication data received by one of the multiple users to enrollment authentication data corresponding to the one of multiple users and received from the depository system, thereby producing an authentication result;

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users, performs cryptographic functions on behalf of the one of the multiple users using at least said private key received from the depository system; and

a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine.

– Claim 2[12]

Applicants note that Claim 2 is the independent claim from which Claims 5 and 6 depend, although the Examiner's explanation suggests that these claims depend on Claim 1. Applicants further note that not all of the elements of the claims are taught. In particular, as previously noted, Examiner's assertion that *Okumara* teaches "enrollment authentication data" is incorrect. The digital certificates of *Okumara* are generated by the system. ("[A] digital certificate [is] issued to the entity." Abstract, *Okumara*) In contrast, the claim calls for "enrollment authentication data" which "identifies one of the multiple users." A comparison of "authentication data ... to enrollment authentication data" is made and "an

---

[12] Claims 5 and 6 are dependent on independent Claim 2.

authentication result" is produced. *Okumara* does not teach this. Thus, the cited reference does not teach at least this element of the claim.

Schneier as a secondary reference fails. The cited portion of *Schneier* also does not remedy the deficiencies of *Okumara*. Assuming, *arguendum*, that *Schneier* teaches "enrollment authentication data," there is no motivation to combine the two references. In particular, the Examiner has not asserted that there is any similarity between the computer game system of *Schneier* and the secure key mapping and aliasing system of *Okumara* or any motivation in these references to combine the two. As explained above, the digital certificate produced in *Okumara* is for use in third party authentication. In contrast, *Schneier* addresses itself to the problem of player substitution at the user interface. Thus, one of ordinary skill in the art of secure key mapping and aliasing would not be motivated to combine *Okumara's* teachings with those of *Schneier*. Assuming *arguendum* that *Schneier* teaches what is missing from *Okumara* the combination is impermissible hindsight reconstruction. *In re Civitello*, 52 C.C.P.A. 865, 869 (C.C.P.A 1964) Thus, there is absolutely no suggestion, teaching, or motivation to obtain the claimed invention. The cited references, therefore, do not render claims 5 and 6 obvious.
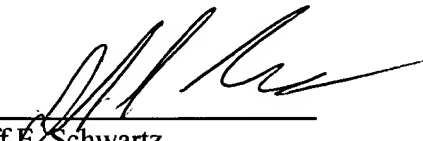
Applicant has properly stated, traversed, accommodated, or rendered moot each of Examiner's grounds for rejection. Applicant submits that the present application is now in condition for allowance.

If the Examiner has any questions or believes further discussion will aid examination and advance prosecution of the application, a telephone call to the undersigned is invited. If there are any additional fees due in connection with the filing of this amendment, please charge the fees to undersigned's Deposit Account No. 50-1067. If any extensions or fees are not accounted for, such extension is requested and the associated fee should be charged to our deposit account.

Respectfully submitted,

10 March 2004

Jeff E. Schwartz
Reg. No. 39,019

Preston Gates Ellis & Rouvelas Meeds LLP
1735 New York Ave., N.W.
Washington, DC 20006
Telephone: (202) 628-1700
Facsimile: (202) 331-1024